

**课 程 设 计 报 告**

**题目： 密码学课程设计**

**课程名称： 密码学课程设计**

**专业班级： 信息安全1805班**

**学 号： U201810679**

**姓 名： 蒋树齐**

**指导教师： 刘铭**

**报告日期： 2020年10月15日**

**教师评语：**

**分数：**

**网络空间安全学院**

密码学课程设计总评成绩

|  |  |  |  |
| --- | --- | --- | --- |
| 完成情况 | 课程报告 | | 总评成绩 |
| （80%） | 格式规范（10%） | 内容完整 （10%） | 100% |
|  |  |  |  |

密码学课程设计任务书

|  |
| --- |
| 课题内容：  （1）原始SPN（教材上）算法的实现。  （2）对上述算法进行线性密码分析及差分密码分析（求出所有32比特密钥）。  （3）增强以上SPN的安全性（如增加分组的长度、密钥的长度、S盒、轮数等）。  （4）对原始及增强的SPN进行随机性检测，对检测结果进行说明。  （5）生成RSA算法的参数（如p、q、N、私钥、公钥等）。  （6）快速实现RSA（对比模重复平方、蒙哥马利算法和中国剩余定理）。  （7）利用椭圆曲线密码算法、HASH函数、压缩函数、对称加密算法实现一个类似PGP的文件加解密及完整性校验功能。  （8）利用USBKEY和数字证书实现简单的文件加密保护。  （9）构造彩虹表破解HASH函数。 |
| 课题任务要求：   1. 掌握线性、差分分析的基本原理与方法。 2. 体会位运算、预计算在算法快速实现中的作用。 3. 可借助OpenSSL、GMP、BIGINT、FLINT等大数运算库的低层基本函数（加、减、乘、除、模），实现过程中必须体现模重复平方、中国剩余定理和蒙哥马利算法的过程。内容(7)的算法可以直接调用OpenSSL或者其它密码库。 4. 了解和掌握彩虹表构造的基本原理和方法，能够设计和实现约化函数（Reduction Function），针对特定的HASH函数构造彩虹表，进行口令破解，了解彩虹表的弱点及防范方法。 5. 独立完成课程设计内容，现场演示并讲解。 6. 掌握USBKEY和证书的基本使用方法。 7. 课程设计完成后一周内，提交课程设计报告。 |
| 主要参考文献（由指导教师选定）   1. 密码学原理与实践（第三版）. DouglasR.Stinson著，冯登国译，电子工业出版社，2009 2. 应用密码学：协议算法与C源程序（第二版）. Bruce Schneier 著，吴世忠等译，机械工业出版社，2014 |
| 同组设计者 无 |

**目录**

[一．实验任务](#_Toc758207207)

[1 SPN算法实现](#_Toc20566751)

[1.1实验要求](#_Toc2068000537)

[1.2实验过程及代码片段](#_Toc2009682311)

[1.3 实验结果分析](#_Toc1107800961)

[2 线性分析](#_Toc127532037)

[2.1实验要求](#_Toc242266153)

[2.2实验过程及代码片段](#_Toc138238759)

[2.3 实验结果分析](#_Toc1949000106)

[3 差分分析](#_Toc1276713851)

[3.1实验要求](#_Toc73092933)

[3.2实验过程及代码片段](#_Toc112278847)

[3.3 实验结果分析](#_Toc1579939463)

[4 SPN增强](#_Toc407259486)

[4.1实验要求](#_Toc779798213)

[4.2实验过程及代码片段](#_Toc2123351897)

[4.3 实验结果分析](#_Toc292087033)

[5 RSA参数计算](#_Toc2106630236)

[5.1实验要求](#_Toc571488363)

[5.2实验过程及代码片段](#_Toc1458047557)

[5.3 实验结果分析](#_Toc469394582)

[6 模重复平方](#_Toc1407304243)

[6.1实验要求](#_Toc177524043)

[6.2实验过程及代码片段](#_Toc791805018)

[6.3 实验结果分析](#_Toc2058260714)

[7 中国剩余定理](#_Toc1521234322)

[7.1实验要求](#_Toc1592432319)

[7.2实验过程及伪代码](#_Toc2068776519)

[7.3 实验结果分析](#_Toc19226256)

[8 蒙哥马利](#_Toc1013137542)

[8.1实验要求](#_Toc404831331)

[8.2实验过程及伪代码](#_Toc771986421)

[8.3 实验结果分析](#_Toc1827066220)

[9 PKCS#7](#_Toc633291087)

[9.1实验要求](#_Toc794344677)

[9.2实验过程及伪代码](#_Toc1792636587)

[9.3 实验结果分析](#_Toc1795033946)

[10 彩虹表](#_Toc1285257366)

[10.1实验要求](#_Toc1930028836)

[10.2实验过程及伪代码](#_Toc254158717)

[10.3 实验结果分析](#_Toc300582736)

[二．实验总结](#_Toc1012506208)

**#蓝色代码片段为伪代码展示思路，黄色代码片段为实际源代码**

# 一．实验任务

## 1 SPN算法实现

### 1.1实验要求

内容：按照教材例3.1实现SPN加解密函数。  
要求：（1）正确实现算法的加解密过程。

（2）快速实现算法。

### 1.2实验过程及代码片段

1. 代码片段（并非实际源代码，仅作为思路展示）



图 1 SPN算法的基本思路

1. 实验过程

了解书上的SPN过程，每一轮轮密钥加的输入是上一轮spn的结果，令其为wi（i=0…n,n为spn的轮数），wi等于明文输入x。轮密钥加的结果为ui，ui分为4部分进行s盒变换后重新合并得到结果为vi，vi将作为下一轮spn输入的wi。

2.轮密钥编排

第r轮密钥Kr为由所给的密钥K（k1，k2，…,kn）,中从k（4\*r-3）开始的16个连续的比特组成。

1. 代码编写

结合上述思路，构造S盒和P盒，主要运用位运算的知识，即可实现SP的功能了，难点在于通过OJ的限制。

### 1.3 实验结果分析

该实验的难度较低，核心思想是阅读教材即可理解并直接上手的，基本功能的实现较为轻松，但OJ的时间限制机制会增加该实验的难度，我也在这个问题上卡了很久。

相关优化：

1. 轮密钥计算函数的优化，由于算法较为简单，直接使用单个表达式计算出结果并return，优化了之前使用太多局部变量和运算的时间和空间。
2. S盒代换的优化，直接使用单个位运算实现最快的代换。
3. 快速读取优化，由于scanf函数太慢，自己写出一个scan函数用于接收字符串，能大幅度加快程序的运行速度。

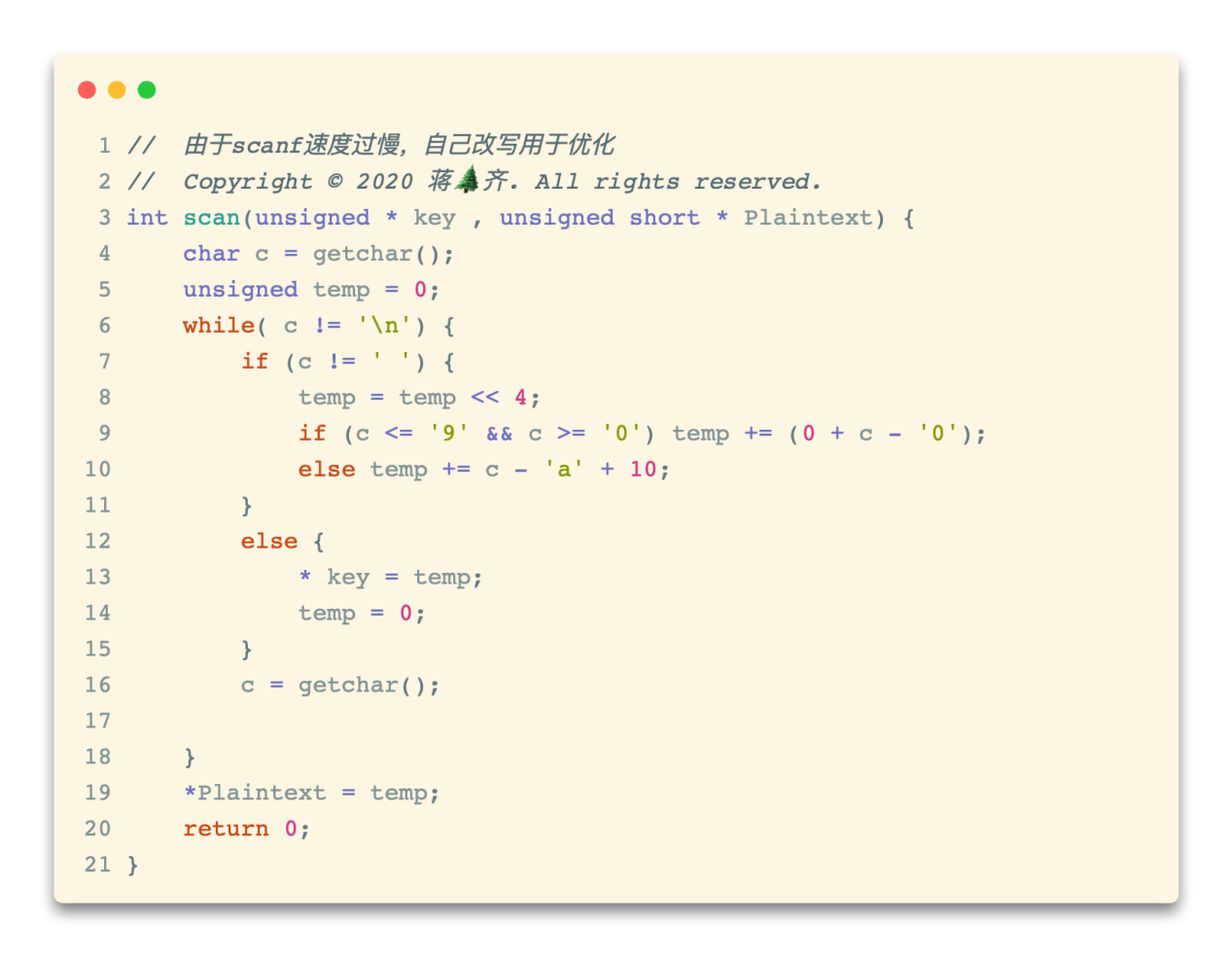
关于快速读取的优化是我这次实验花的最多的精力的位置，使用scanf时最后一个监测点永远是2200ms，距离2000ms的标准还差了很多，使用快速读取后直接优化到1100ms，快了整整一倍。下面给出快速读取scan函数的源代码用于参考。

图 2 快读函数的源代码

## 2 线性分析

### 2.1实验要求

内容：根据已知明密文对分析原始SPN的密钥。  
要求：（1）实现教材所给算法。

（2）能根据所给8000对明密文对分析对应位置密钥。

（3）分析出所有32比特密钥。

### 2.2实验过程及代码片段

1. 代码片段（并非实际源代码，仅作为思路展示）



图 3 线性分析函数的思想

2.选择的线性链及其来源  
 一号链：x5 ^ x7 ^ x8 ^ u6 ^ u8 ^ u14 ^ u16

二号链：x5 ^ x6 ^ x7 ^ x8 ^ u2 ^ u4 ^ u6 ^ u8 ^ u10 ^ u12

两条链的来源：第一条链为书上所给的链偏差为1/32，第二条链是结合年纪交流群里6班的王耀辉同学的提示找到的，链偏差为1/16。第一条链可以分析出最后一轮轮密钥的5-8位bit，13-16位bit，第二条链需要在得到第一条链的基础上分析得到最后一轮正确密钥的1-4，9-12位。

3.线性链破解过程

对所给的输入明文密文以及假设的密钥计算一号链的异或值，得到结果为零则计数器加1，计数器值减去样本数T的一半取绝对值的值（简称最大计数值，同理有计数值概念）最大的密钥有可能成为正确密钥。当得到正确的16位密钥后暴力搜索剩下16位密钥即可得到结果。

### 2.3 实验结果分析

实验整体较为顺利，可能是借助了年级群里同学提供的第二条链的原因，最开始一直超时最后的点，修改了几处循环后，明显提速，调用了memset函数进行了计数数组的初始化，速度明显加快。

加快速度的同时也因为memset函数的问题一直出现Time Limit Exc的问题，就是因为menset函数中一个参数的错误，导致我的存储密钥的数组也被一并初始化，导致数据的丢失，修改后即可通过所有任务点。

## 3 差分分析

### 3.1实验要求

内容：根据已知明密文对，选择明密文分析原始SPN的密钥。  
要求：  
（1）实现教材所给算法。  
（2）能根据所给明密文对分析对应位置密钥。  
（3）分析出所有32比特密钥。

### 3.2实验过程及代码片段

1.代码片段（并非实际源代码，仅作为思路展示）



图 4 差分分析函数的思想

2.选择的差分链  
一号链：输入异或：0x0B00 输出异或：0x0606

二号链：输入异或：0xf0f0 输出异或：0x8088

3.差分链破解过程

对所给的每对满足输入异或明文密文进行判断是否为正确对，若为正确对则枚举密钥，每个密钥赋予一个计数器，当输出异或正确时，计数器值加一。当所给正确对数满足需求时，对所得密钥进行暴力搜索得到剩余16位密钥。

### 3.3 实验结果分析

在通过了线性分析后，这一题就显得相对容易，还是对于链的寻找加上一部分的暴力搜索。此题目在有了前面实验的Time Limit Exc超时教训之后，直接采用了前面的使用的一些思想，比如快速读取，位运算，故顺利通过该实验。

## SPN增强

### 4.1实验要求

内容：对原始SPN进行改进。  
要求：  
（1）选择合适的密钥长度、分组长度、S盒、P置换、轮数。  
（2）效率较高  
（3）输出达到随机数检测标准

### 4.2实验过程及代码片段

1. 代码片段

图 5 SPN增强的思想

1. 实验中借用的S盒与P盒

以在下图给出，为了达到OJ上的随机要求，使用三轮，以下的代码均取自教材P76页。

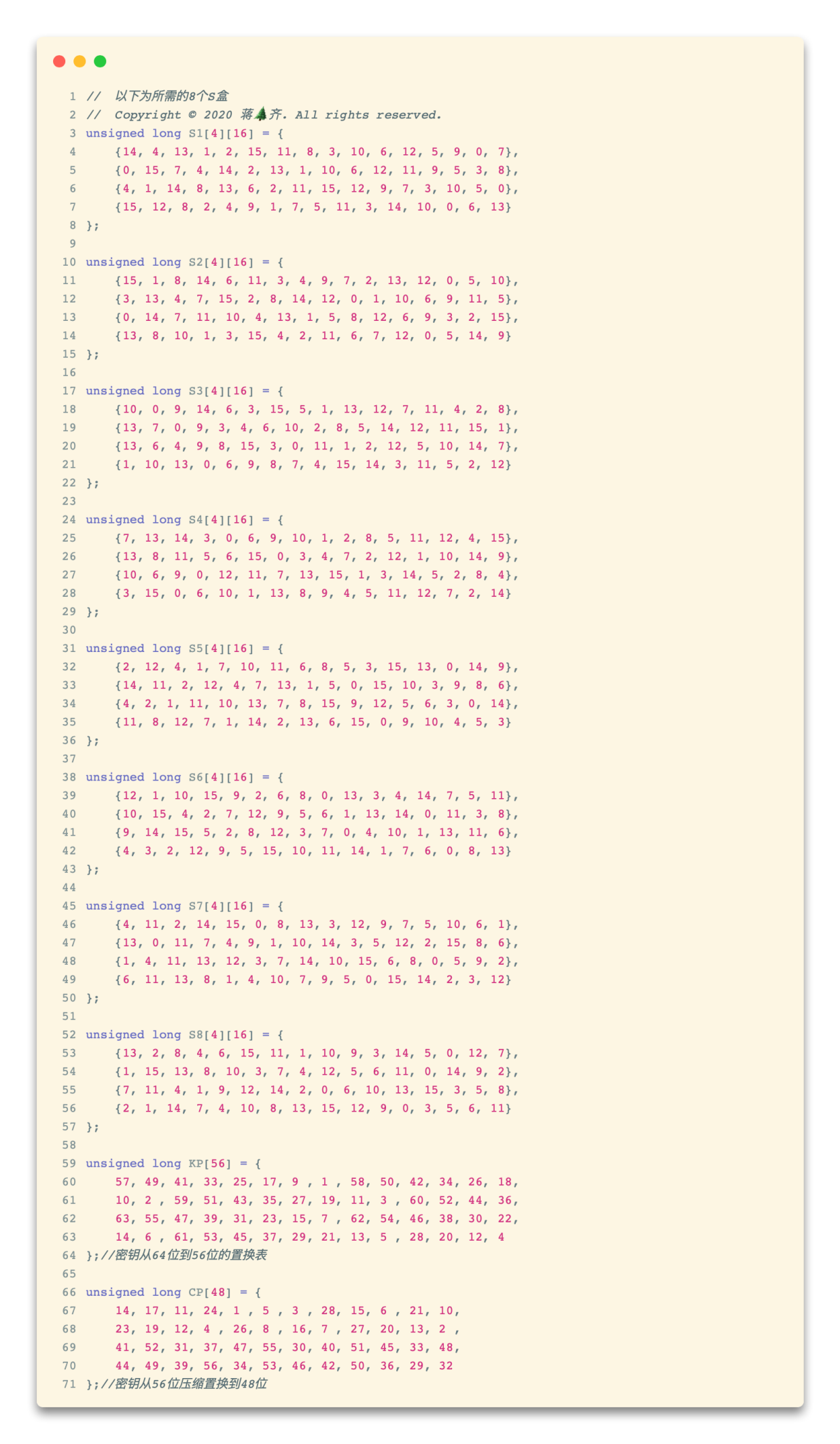


图 6 SPN增强用到的盒

### 4.3 实验结果分析

为了满足OJ的随机数要求，测试得到3轮DES可以通过，并且该实验的输入模式为CBC模式，与上三个实验不同，需要格外留心。

## 5 RSA参数计算

### 5.1实验要求

内容：求RSA参数d。

要求：

（1）利用加法、减法、乘法、模运算等基本运算。

（2）自己实现求逆,gcd

（3）简单检查参数的合法性

### 5.2实验过程及代码片段

该实验借助了GMP库进行大数据运算，需要满足的要求很多，并不是简单求出RSA的d即可。实验的代码片段如下：

1. 辗转相除法求逆。

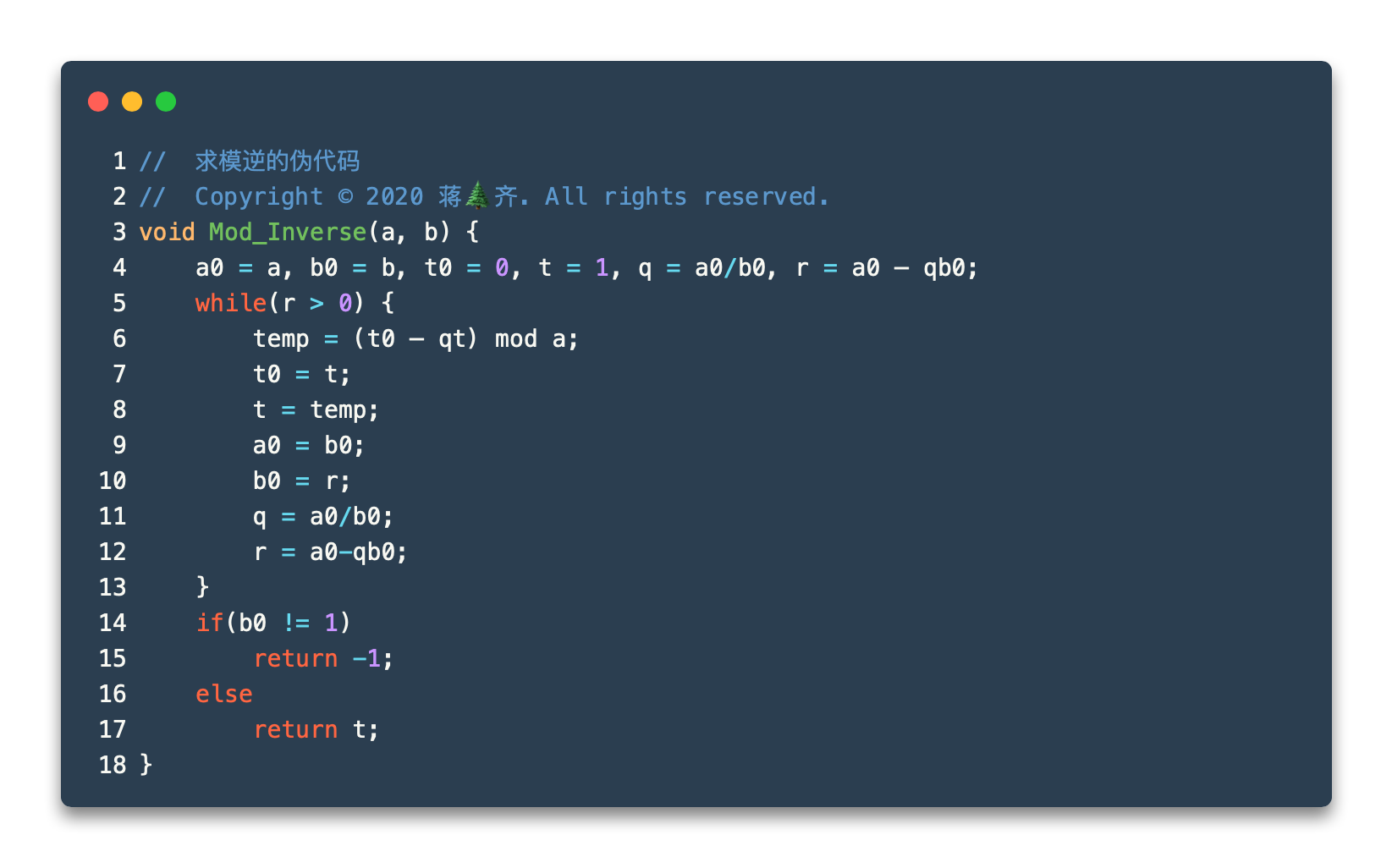


图 7 辗转相除法求逆的基本思路

1. 求最大公因数。

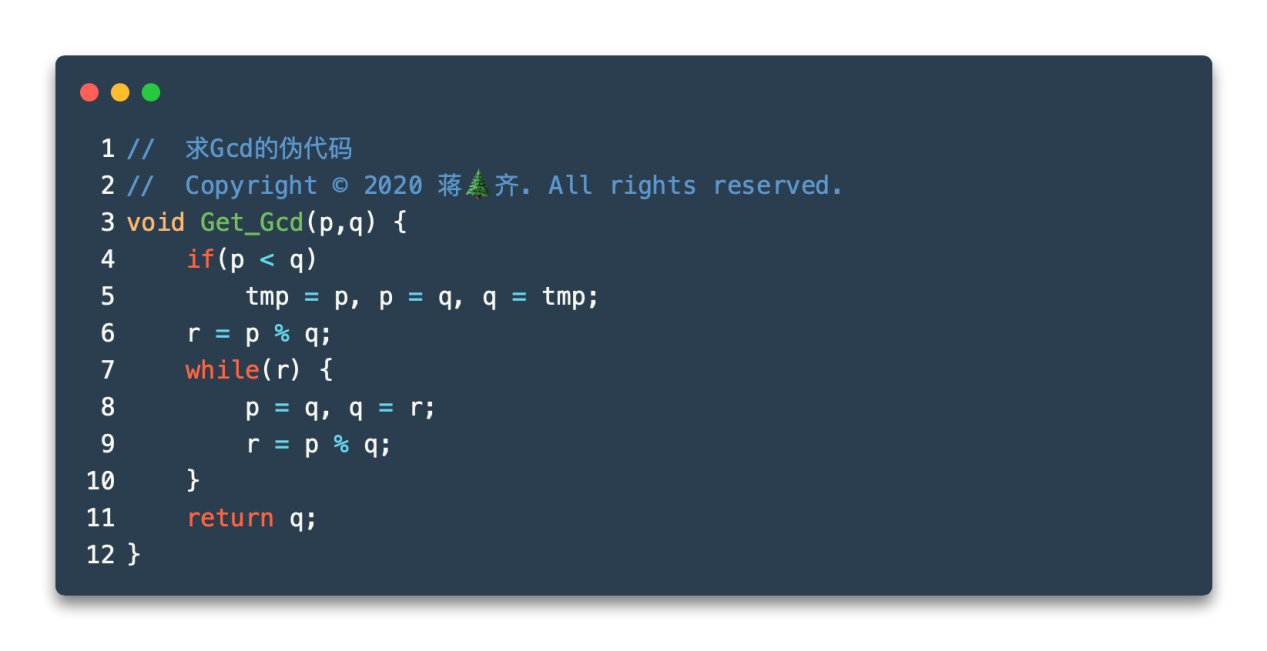


图 8 求最大公因数的伪代码

### 5.3 实验结果分析

实验中需要注意以下四点：  
1.p，q是否为素数，可用拉斯维加斯算法进行运算。

2.p，q的差值是否国小，题目中经过尝试当p，q差值大于1000时会提示正确。

3.e是否较小，若较小，则可能会容易被攻击成功。

4.p，q是否有小因子，若存在小因子，被攻击成功概率也较大。

## 6 模重复平方

### 6.1实验要求

内容：正确计算a^e(modN)。  
要求：

1. 利用加法、减法、乘法、模运算等基本运算。

（2）自己实现expmod(a,e,n)

### 6.2实验过程及代码片段

1. 代码片段如下

使用gmp库的函数实现以下思路即可。

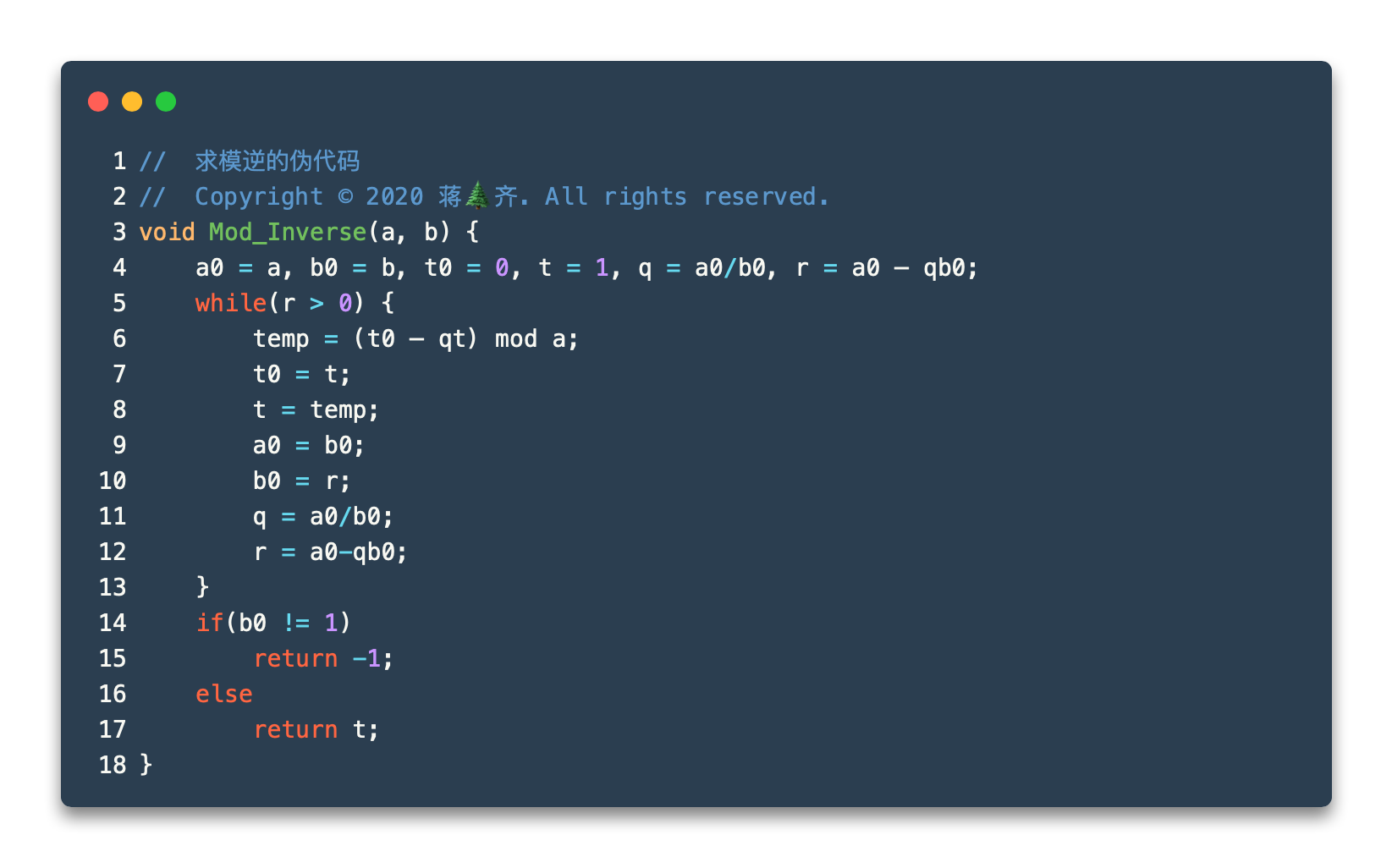


图 9 求模逆的伪代码

### 6.3 实验结果分析

这一题相对较为简单，采用上述的模重复平方算法，在每次底数相乘时模n可以简化运算加快速度。较为容易通过OJ，需要纠结的是是否使用mpz\_t的整数方法，但是会变得很繁琐，但是不使用又会降低代码的运行速度。

## 7 中国剩余定理

### 7.1实验要求

内容：正确计算c^d(modpq)。  
要求：

（1）利用V中的求逆运算从加密密钥e计算解密密钥d。  
（2）利用VI中实现的模幂运算和中国剩余定理计算c^d(modpq)。

### 7.2实验过程及伪代码

1. 中国剩余定理代码片段如下



图 10 中国剩余定理的基本思路

//中国剩余定理最终乘法

m = m1\*q\*p^(-1)mod(q) + m2\*p\*q^(-1)mod(p)

### 7.3 实验结果分析

遇到的问题主要是无法通过OJ的时间限制，可以进行如下优化

模幂应采用高位往低位的64进制快速模幂算法。这个方法的关键在于用多个2进制位合成一个k进制“位”，一次处理k个2进制位，预处理过程需要进行2^k-1次模乘(由于2进制转k进制，原来第五个问题中由高位往低位乘的g就存在64种可能)，预处理花费的时间相对于减少模乘次数减少的时间是十分之少的。运算过程大约需要进行n次模平方和n/k​次模乘。不难看出，减少模幂过程的运算次数主要是减少模乘的次数，模平方的次数总为n次。

## 8 蒙哥马利

### 8.1实验要求

内容：正确计算a^d(modpq)。  
要求：  
（1）实现Montgomery算法。  
（2）Montgomery+中国剩余定理

### 8.2实验过程及伪代码

1. 滑动窗口的快速幂算法（以下为实际源代码）

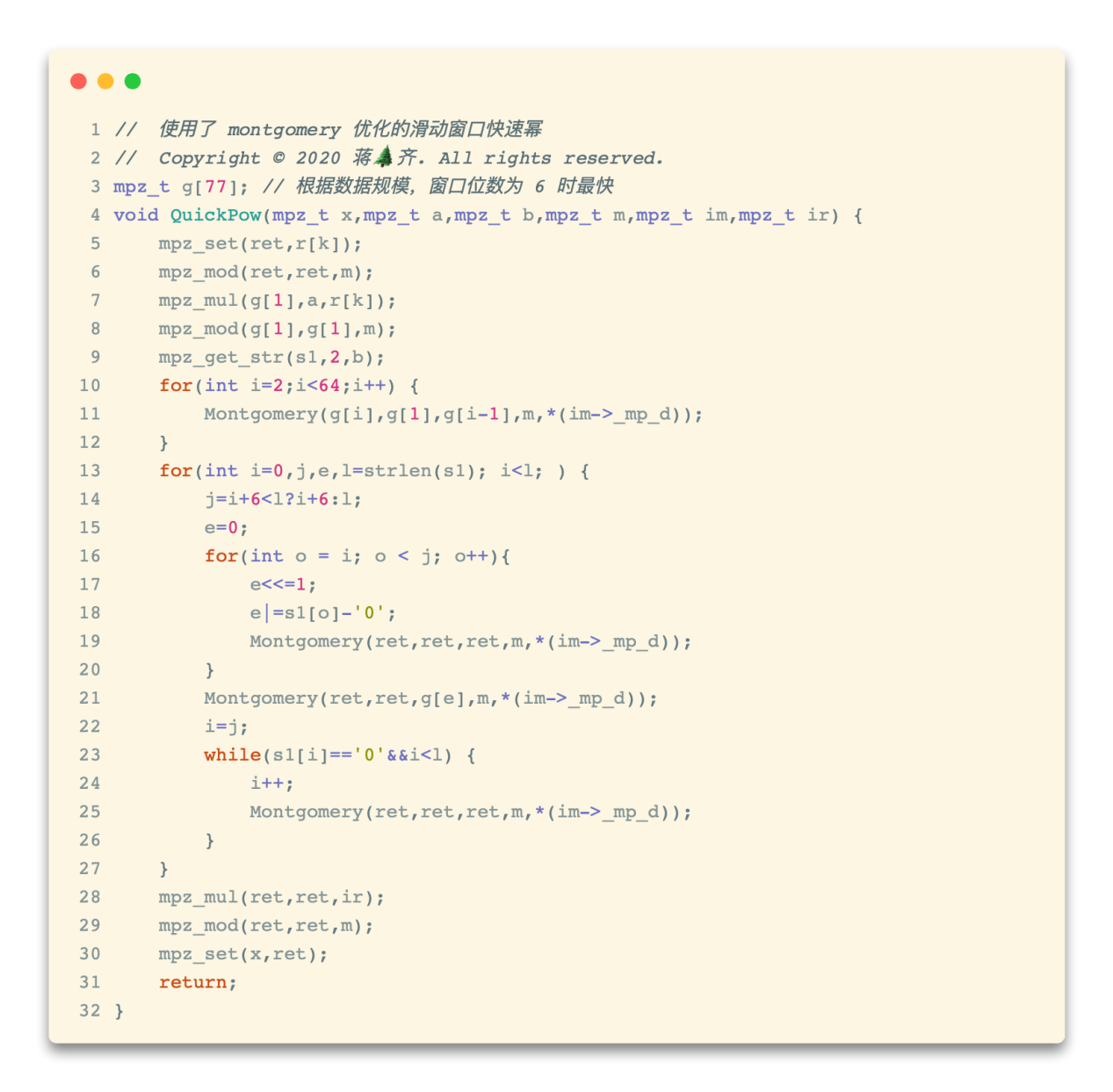


图 11 滑动窗口的源代码

2.算法出处，来源于NodeBB上一位同学分享的方法

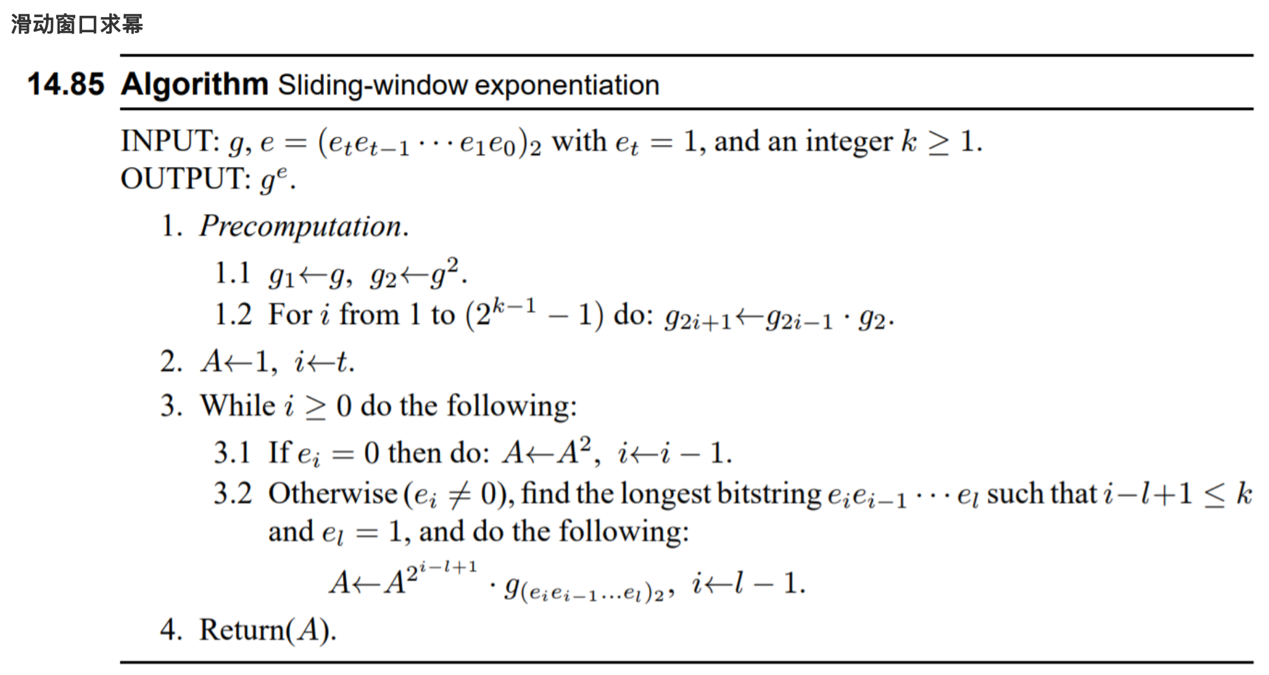


图 12 参考的伪代码

### 8.3 实验结果分析

实验的实现并不困难，困难的事加快速度达到OJ的标准。

使用普通的快速模幂算法并不能通过所有测试点，为了降低模乘次数采用64进制的快速模幂。

## 9 PKCS#7

### 9.1实验要求

内容：PKCS#7是PKI中用于消息加密的语法标准。可以用于给拥有公钥的用户发加密邮件、传送加密文件等。现在假设我们有一个可信的根CA，用户B是PKCS#7格式加密消息的接收者，用户B私钥题目已给出，输入发送者A发送的PKCS#7格式的信息。我们需要解开PKCS#7的包装，完成验证A身份合法性，信息完整性，解密提取A发送消息的任务

### 9.2实验过程及伪代码

1.安装gmssl编程环境

在ubuntu18.04中完成gmssl安装，将编译好的的gmssl中的所有.a和.so文件链接到编译器内。

2伪代码



图 13 PKCS7的主体思路

### 9.3 实验结果分析

这个实验确实是最让人两眼一抹黑的实验，从完全不知道从何做起看不懂题目到最终完成花了很长的时间，过程中1801班的李文科同学给予了我很大的帮助，他参考了老师写好的源代码完成了代码编写，并给我提供了同样的思路。

这题的难点在于涉及了很多C++的知识和openssl库的知识，需要自己去查阅库函数的功能来凭凑要实现的目的，也增强了对x509证书的了解。

题目的描述显得实验极其复杂，但当阅读完老师写好的代码的思路，并查阅了函数功能之后，算法的实现并不是特别困难。

## 10 彩虹表

### 10.1实验要求

内容：已知SHA1彩虹表的100个R函数其中i=1,2,3,...,100。

现在有一些链头和链尾，每条链从链头开始，依次调用了100000次SHA1和R函数得到链尾。希望从这些链中找到SHA1值对应的口令

### 10.2实验过程及伪代码

1.代码片段



图 14 彩虹表所需的函数伪代码

### 10.3 实验结果分析

前100（不到100次）走步操作对应着输入hash值的下一次可能R操作，总共约有100\*100000次走步和验证操作。由于整个算法过程R函数需要进行多次，故将R函数中对字母的比较和转换换成字典读取的方式会更快。

题目所给的getstr函数可以将数字所代表的字符先提前存入一个字符数组，即可完成字典方式的读取大大提高运行速度。

# 二．实验总结

这是一次印象深刻的课程设计，与其说是课程设计，不如说是分级通关，OJ的出现给这次实验带来的不同之处就是，你不仅仅需要完成实验任务书上要求的任务，还要根据自己的理解进行代码的优化，时间的限制让我真正切切实实把C语言课堂上学到的优化知识拿来使用，尝试“用空间换取时间”。

再被优化问题折磨的同时，我也强化了对密码学的理解，深刻的感受到密码学原理与实践的实践部分。

对于C函数的理解也有了更深刻的认识，例如scanf的底层实现，这也是第一个SPN实验给我留下的最深刻的印象，在自己写快读函数之前，最后一个数据点的耗时为2200ms，在使用了快速读取之后，速度直接快的超乎想象，来到了1100ms，直接快了一倍，于是后面几乎所有的实验，我都使用了自己的快速读取函数，也特意将其源代码放在了实验一的分析结尾中。

再回到这次实验的核心，密码学。

亲自实现了SPN置换代换网络，感受到了密码学的核心思想，制造混乱。但制造混乱的方式会给破译留下线索。

让我印象最深刻的就是线性分析的实验，也是我花了时间最长的实验，这是一个基于概率论基础的密码攻击，通过概率基础得到部分信息，缩小穷举需要的工作量，要知道一位bit的确定都会对枚举的工作量带来指数级别的减少。而且对于密码学的学习不能只停留在对已知攻击的了解，更应该去理解攻击的理论核心是什么，去理解表层代码下的深层含义，去提升自己遇到其他问题时候的思考能力和判断力。

再说说印象也很深的一部分，GMP库，这也是第一次我面对庞大的信息量进行有效信息的筛选，面对一个全是英文的网站一点点翻找自己需要的函数，需要的对象和方法，查找底层函数，通过OJ对时间的限制。

同时一到三班一些同学的思考也值得我们学习，在OJ的NodeBB平台上，就有同学分享了很多种快速模幂的算法，这种不仅局限于通过OJ，而是发掘新的算法学习新的知识的态度同样是值得学习的，在Montgomery算法的实验中，我就参考了上述同学分享的滑动窗口快速模幂算法，并根据实际问题找到了最合适的K进行优化。

这次实验的过程于我而言更是一个不断探索未知的过程，在面对困难问题时摆正心态，不逃避，迎难而上，网上没有现成的教程，你就当第一个做出来的人，同时这次课程设计也让我感受到了理论和实践的距离是需要亲自感受才能弥补的，不能只拘泥于书上的理论，实践才是一个华中大学生该有的作为，要在实践中不断摸索，真正做到“明德厚学，求是创新”！